

REMARKS

In the Official Action mailed on **12 November 2008**, the Examiner reviewed claims 1-2, 4-6, 8-10, 12-14 and 16. Examiner rejected claims 1, 4-6, 8-9, 12-14, and 16 under 35 U.S.C. § 103(a) based on De Vries (U.S. Patent No. 6,928,428, hereinafter “De Vries”), and Hild et al. (U.S. Patent No. 6,763,440, hereinafter “Hild”). Examiner rejected claims 2, and 10 under 35 U.S.C. § 103(a) based on De Vries, Hild, and Turvey (U.S. Patent Application No. 2002/0019849, hereinafter “Turvey”).

Rejections under 35 U.S.C. §103

Examiner rejected claims 1 and 9 under 35 U.S.C. § 103(a), asserting that these claims are unpatentable over De Vries in view of Hild. Applicant respectfully disagrees, because neither De Vries, nor Hild, nor any combination of the two, disclose either explicitly or implicitly a system wherein the item of private information is received at the database in plain text, and the hash of the item of private information is created by the database in a manner that is transparent to an application which manipulates the private information.

Specifically, De Vries discloses a system wherein:

In one embodiment of the invention illustrated herein, the black box takes the form of a set of query, answer pairs, where the query hash is represented as a hash result that is a one-way hashing function of a set of query input values. This set of query, answer pairs is distributed to other computers which can then effectively query the confidential information without having access to or directly processing the raw confidential information. (De Vries, Col. 2, Lines 7-14)

In this system disclosed by De Vries, the **hash is calculated on a trusted computer**, and the **hash is then sent to the database**, possibly on an untrusted network. De Vries is concerned with solving the problem where untrusted providers perform queries with private information, and thus discloses a system where the private information is hashed prior to sending it to the database on the untrusted system.

In contrast to De Vries, embodiments of the present invention provide a system wherein the item of private information is received in plain text, and the **hash of the item of private information is created by the database** in a manner that is transparent to an application which manipulates the private information. The present invention is not concerned that the item of private information is revealed to the database, but rather, does not want the private information stored in the database in a manner that the private information can subsequently be revealed.

Thus, De Vries teaches away from the present invention wherein the hash of the item of private information is created by the database in a manner that is transparent to an application because De Vries teaches that the private information is hashed prior to delivering it to the database.

Accordingly, Applicant has amended claims 1 and 9 to clarify that the hash of the item of private information is created **by the database** in a manner that is transparent to an application which manipulates the private information. These amendments find support in claims 3 and 11 of the instant application. Support for these amendments can be found in paragraphs [0020] and [0021] of the Instant Application.

Hence, Applicant respectfully submits that independent claims 1 and 9 as presently amended are in condition for allowance. Applicant also submits that claims 2, 4-6 and 8, which depend upon claim 1, and claims 10, 12-14 and 16, which depend upon claim 9, are for the same reasons in condition for allowance and for reasons of the unique combinations recited in such claims.

CONCLUSION

It is submitted that the present application is presently in form for allowance. Such action is respectfully requested.

Respectfully submitted,

By /Shun Yao/
Shun Yao
Registration No. 59,242

Date: 12 March 2009

Shun Yao
PARK, VAUGHAN & FLEMING LLP
2820 Fifth Street
Davis, CA 95618-7759
Tel: (530) 759-1667
FAX: (530) 759-1665
Email: shun@parklegal.com